2003

A Case Study in the Security of Network-Enabled Devices

Simeon Xenitellis

Craig Valli
Edith Cowan University

A Case Study in the Security of Network-Enabled Devices

Symeon (simos) Xenitellis
Information Security Group, Royal Holloway, University of London, UK
s.xenitellis@rhul.ac.uk

Craig Valli
School of Computer And Information Science, Edith Cowan University, Australia
c.valli@ecu.edu.au

Abstract: It is becoming increasingly common for appliances and other electronic devices to be network-enabled for usability and automation purposes. There have been fears that malicious users can control such devices remotely. Since the installation base of such network-enabled household devices is still relatively small, we examine the types of vulnerabilities that another such appliance has, the network-enabled printer, which is commonly found in the education and business sector. In this paper we analyse the source of the vulnerabilities and present detailed threat scenarios. In addition, we examine four organisations in Australia and Europe. Based on the results of the case study, we draw conclusions on the effects of an information warfare attack using network-enabled devices as the medium.

Keywords: information warfare, network-enabled devices, network printer, information warfare, security

1. Introduction

A network-enabled (or network printer) printer is a typical electronic document printer that also has a network interface (Ethernet port) allowing it to be connected directly to a Local Area Network (LAN) of an organisation. The ability to connect directly requires the existence of an Embedded Operating System (EOS) in the network printer. The EOS usually comes with value-added services, such as configuration through a WWW interface, for purposes of usability and functionality.

When a user installs a network printer, these value-added services are typically enabled by default. Simply connecting the device to the LAN enables the users to configure and print documents quite easily. For example, connecting with the Internet browser to the printer allows the installation of the appropriate printer driver, as shown in **Figure 1**.

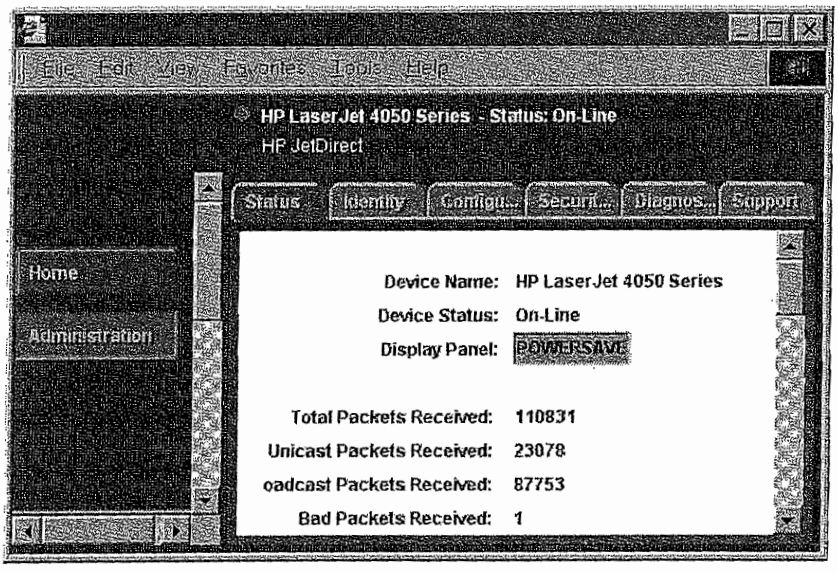

Figure 1 WWW Configuration and Installation of a network printer, page provided by printer device.

In **Figure 1**, the EOS makes available by default a Web server where users can connect using their Web browser and manage the device. Typical tasks are the installation of the appropriate drivers for the client computer and the basic management of the device. In addition, using specialised administration software, the user is able to control fully the device from a remote location. Both the basic and full administrative modes are available by default with no access controls.

It is common not to restrict the access to the network devices in an organisation for different reasons. A common reason has to do with organisational structures and politics. Scant network resources such as network printers typically fall within a departmental jurisdiction and are considered the resources of that department. It is not uncommon for departments to have specialist requirements for printing that require specialist printers. These printers are then "owned" by the particular department. The department is responsible for maintenance and configuration, which is often done by a third party typically the supplier who installs the default settings. Due to the nature of printing requirements and scarcity of the resource it is rare to see organisational-wide network management being used to manage all such devices. In cases that there is restriction to the access, there exist several alternative access protocols that effectively allow the same functionality. Hence, the possibilities for vulnerable devices are high.

In this paper we examine what kind of functionality is available in the form of the availability of basic functionality (primitives) that an attacker can make use of, in order to disrupt services. Furthermore, we examine four organisations with regard to the availability of network-enabled printers. In addition, we analyse threat scenarios for distributed denial of service attacks.

The rest of this paper is laid out in six sections. In Section 2 we provide background to services available to network devices. In Section 3 we discuss related work on attacks against network-enabled devices. In Section 4 we analyse the potential types of attacks focusing on the primitives offered by the devices while in Section 5 we present our experimental results. In Section 6 we present threat scenarios. In Section 7 we provide countermeasures and end in Section 8 with conclusions.

2. Background

Electronic devices provide increasingly more functionality to the consumers for a variety of reasons, such as market differentiation, enhanced functionality and usability, and modular design. In order to cut costs, it is common for manufacturers to use off-the-shelf components to assemble the device often from the same originating manufacturer. For example, instead of programming the device in a low level programming language, higher-level languages are used such as C and Java. In addition, embedded operating systems have become a commodity and are available by specialised vendors with a wide list of specialised features. These features are available by default and there is a common access interface among different manufacturers.

We can assume that a manufacturer would normally opt to keep enabled all the access protocols available to the device, as they are normally included in the TCP/IP stack of the network operating system and for ease of end-user installation of the device. As an example, a specific network printer has more than ten different services active (Hewlett Packard, 2003).

For network administration tools to be able to access all network devices in an organisation, the latter should require either default known passwords or no passwords at all. An example of the output of such an administrative tool is shown in Figure 2. It shows the results of an automated discovery session. For each device found, further administrative tasks can be performed, such as updated the device software and firmware.

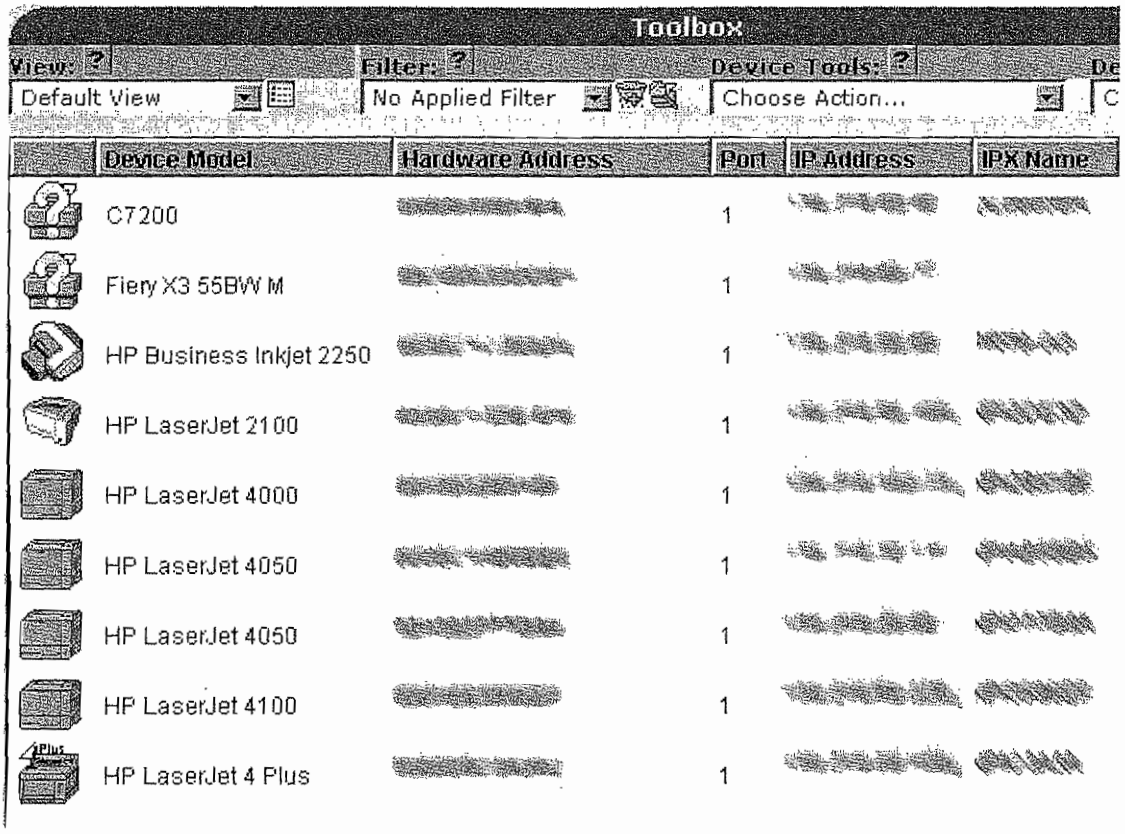

Figure 2 Using a discovery tool to locate active network devices.

These access protocols have access control mechanisms (such as restricting access based on the source IP address) or require authentication. Due to the variety of the access control mechanisms, it is expected that in the majority of the devices no protection is enabled.

In this paper we describe as *PJL protocol* the protocol that uses the network port 9100 and accepts commands that conform to the PJL language (Hewlett Packard, 1997), which is an industry standard. The issue arises from the fact that Hewlett Packard does not provide any name for the resulting protocol in the documentation. The *PJL protocol* has wide acceptance and is among the most common protocols for network printing along with the Internet Print Protocol (deBry et al, 1999).

3. Prior work

In (FX et al, 2002), the authors describe generic attacks against network devices providing proof-of-concept implementations. Using these implementations, one can verify in practice specific types of vulnerabilities. Part of their discussion on network devices is network-enabled printers. In addition, drawing from resources such as public security mailing lists and security WWW sites, we summarise these attacks in the following categories:

- Different access protocols exist with separate access control mechanisms. If a specific functionality is disallowed in one protocol, it may not have been disallowed in the other protocol.
- Protocols may be able to be configured to require authentication. Apart from the fact that authentication credentials are typically transmitted without encryption, specific protocols may have limitations, which compromise the security. For example, in the PJL protocol the password is a number between 1 and 65535. An exhaustive key search is possible.

- Buffer overruns and other software reliability issues may exist. Although one might expect that software reliability issues cannot be exploited to produce security vulnerabilities such as remote execution of code, there are however, examples that this is possible.
- Network-enabled printers can have a file-system so that files can be stored. This storage can be misused.
- If access controls are not set properly, then it is possible to upload software in order to execute as part of the software or firmware update functionality.

There is a trend to make increasingly more devices network-enabled. In (Valli, 2002) there is such a discussion on the potential of a large-scale automated attack against these devices.

4. Types of attacks

A network printer usually offers a range of network services. Such a list is shown in **Table 1**.

Table 1 Common access protocols found in network printers

Protocol	Port	Use	Comments
FTP	21	Printing	Alternative printing method
Telnet	23	Configuration	Device configuration
Finger	79	Diagnostics	On specific devices only (firmware)
HTTP	80	Configuration	WWW interface to configuration
LPD	515	Printing	RFC 1179
PJL	9100	Configuration; Printing	Uses the PJL language

Potential attacks can target functionality and inadequacies found in the protocols listed in **Table 1**.

```
#!/usr/bin/perl -w
use strict;
use Socket;

my ($remote, $port, $iaddr, $paddr, $proto, $line, $msg);
$remote  = shift || "myprinter";
$port    = shift || "jetdirect";
$msg     = shift || 'READY';
if ($port =~ /\D/) { $port = getservbyname($port, 'tcp') }
die "No port" unless $port;
$iaddr   = inet_aton($remote)               || die "no host: $remote";
$paddr   = sockaddr_in($port, $iaddr);
$proto   = getprotobyname("tcp");

socket(SOCK, PF_INET, SOCK_STREAM, $proto)  || die "socket: $!";
connect(SOCK, $paddr)    || die "connect: $!";
print SOCK "\033%-12345X\@PJL RDYMSG DISPLAY =" .
                    " \"$msg\"\r\n\033%-12345X\r\n";
close (SOCK) || die "close: $!";
exit;
```

Figure 3 Sample application that changes the message "READY" on the LCD display of a network printer.

The sample application in Figure 3 uses the PJL language (Hewlett Packard, 1997) that is supported by a wide range of network printers. With this language, a user can set or read parameters on the network printer or access the internal file-system provided by the system. This example shows how easy it is to use specific functionality of a protocol in order to make an actual implementation (also called an *exploit*). For this sample application, we implemented it, working from an example written in C (mudge, 1999), in less than twenty minutes.

5. Experimental results

We examined four organisations in Europe and Australia as to the number of network printers that are available. The results are shown in **Table 2**.

Organisation	A	B	C	D
Number of active hosts	3742	178	342	278
Number of network printers	86	22	9	13
Protocol PJL	86	3	2	11
Protocol SNMP	85	22	9	13
Protocol HTTP	68	-	4	11
Protocol LPD	66	22	8	13
Protocol FTP	44	-	6	11
Protocol Finger	1	-	2	2

Table 2 Network printers and protocol availability in organisations in Australia and Europe

We can draw a list of conclusions from **Table 2**. Depending on the type of the organisation (education, industry or government), one can expect a population of more than %2 of devices being network-enabled printers. In specific settings with different requirements, this number can be higher as much as %12. In addition, the minimal percentage of %2 typically corresponds to several network devices since a typical organisation has more than 300 IP addressable systems.

In general, the availability of the PJL protocol implies the availability of SNMP, HTTP, LPD (McLaughlin, 1990) and to a lesser extent the FTP protocol. The finger protocol is generally available to a specific brand of network printer.

6. Threat scenarios

We present a list of threat scenarios that can have impacts on the availability, integrity, confidentiality and non-repudiation.

6.1 Mounting an attack

To mount a large-scale attack, the attacker would first need to enumerate the victim systems and identify the subset of those that exhibit the specific vulnerability. One method to accomplish the enumeration is to establish the IP address range of the potential victims and then identify them from a common signature such as the ability to receive print jobs from a specific network protocol. A specialised network program, a *port-scanner*, can be employed to perform this task. A port-scanner essentially attempts to make connections to the systems that we want to check and displays those that are active and have the specific service available. One can use an open-source port-scanner, such as (Fyodor, 2003) and (Vogt, 2003) or write a custom version as part of malicious software.

In Figure 4 we show how the manual command to check a Class C domain would look.

```
# nmap -sS -p 9100 -m output.txt 192.168.1.1/24
```

Figure 4 How to use the NMAP tool to scan a Class C network.

In the file *output.txt* one can identify the systems that respond to connections on port 9100, the standard port for the PJL protocol. This command scans hosts with IP addresses of the form 192.168.1.x, where x = 0 ... 255.

In the following we assume that we have identified the victim systems. We must point out that most of the following attacks are available in their generic form if no protective measures have been taken to protect the network printer.

6.2 Attacks against the availability

An attacker may send special print jobs that consume the consumables of the network printer. For example, sending the file in Figure 5 to a PostScript® printer would print a blank page, wasting the ink or the toner. Adding the directive `/#copies 500 def` would print a 500 pages file of black pages, emptying the paper tray.

```
%!PS-Adobe-3.0
%%BoundingBox: 0 0 595 842
%%LanguageLevel: 2
%%DocumentData: Clean7Bit
%%Pages: (atend)
%%PageOrder: Ascend

%%Page: 0 0
%%PageBoundingBox: 18 18 577 824
0 0 0 setrgbcolor
299 227 1731 2901 rectfill
showpage
%%Pages: 1
%%EOF
```

Figure 5 Sample minimal PostScript® file that prints a single black A4 page.

The remote information warrior could also monitor these types of printer and every X number of prints output a protest banner or slogan to the network-enabled printer. While not as destructive as the previous example can be disruptive and effective at broadcasting information-based operations.

There are documented vulnerabilities that remote attackers can use to render a network printer unusable. The printer in some cases needs a power-cycle to continue working while in other cases the damage is irreparable requiring hardware repair such as exhaustion of the printer drum. We have verified this behaviour in several network printers.

6.3 Attacks against the integrity

A network-enabled printer has typically the functionality to update its firmware and software remotely. This can be exploited to enable the malicious updating of the firmware with a padded image or corrupted image. The net result is that typically the whole printer logic board would be replaced this is typically the most expensive component in a printer.

As described in (FX et al, 2002), an attacker can execute custom code. The examples given were a WWW based port-scanner, a common password cracker and a port redirector. An application of the last, the port redirector is to make a connection to an end system through the printer, thus hiding the real source address. Since no logging takes place, the attacker can achieve a good degree of anonymity.

6.4 Attacks against the confidentiality

Depending on the configuration of the client systems, print jobs (the actual files to be printed, possibly in an intermediate format) may be available on the storage area of the printer, accessible to a potential attacker. One method that this can be achieved is if the job retention option is enabled. Print jobs are stored on the network printer with the possibility to be retrieved by an attacker.

In addition, using the PJL language an attacker can get a list of the print jobs, which includes the names of the files recently printed, and the time they were printed.

6.5 Attacks against non-repudiation

Since a network printer is accessible remotely and no logging information is kept with regards to the origin of the print job, one can repudiate the printing of a potentially controversial document. In this scenario, one can claim that someone else sent the print job.

In the case of a racism case, one may choose to print offensive documents anonymously and not claim them afterwards. In this situation, it is typical for such printouts to stay next to the printer for long before thrown away.

7. Countermeasures

Due to possible jurisdiction issues with regards to the management of network devices, we recommend that the focus of the protection should be placed on IP filtering rather than to enabling access control to each individual device.

Thus, as a first line of defence, an organisation should apply IP filtering for incoming connections to the services listed in **Table 1**. If a firewall is not available to provide IP filtering, then the organisational router should be used to protect these devices.

Where possible intrusion detection systems should also be deployed that track and alert for activity on these ports. The intrusion detection system should monitor for external and suspicious internal traffic e.g. interdepartmental traffic that should not be occurring. Due to the nature of certain attacks filtering of for instance of all black page printer payloads could be intercepted.

In addition, zone transfers of the DNS information of an organisation should be disabled, as they make organisation-specific attacks easier to accomplish. Obviously, this is not a foolproof solution as someone can get the DNS information from alternative sources. However, it adds a level of difficulty for the attacker and in addition it is a recommended step in different security policy manuals.

The use of network printers in a defensive network honeypot design could also yield effective attack intelligence on malicious intruders as well as providing a delay response.

8. Conclusion

We demonstrated that existing network-enabled devices provide ample functionality and if they are not managed securely, allow an attacker to launch an attack against the information infrastructure of an organisation or a segment of the Internet.

In addition, we showed that at least 2% of all IP addressable devices of an organisation are currently expected to be network-enabled printers. For a large organisation with more than 4000 IP addressable devices, the number of network-enabled printers is significant.

Furthermore, we presented threat scenarios against the security of organisations with enough details to evaluate the effectiveness of an attack. The attacks can be against the confidentiality, availability, integrity and non-repudiation.

Finally, we recommend countermeasures giving emphasis to IP filtering to limit the exposure of the multiple active services. The use of intrusion detection systems and defensive honeypots could also prove useful in countering attacks on these types of information infrastructure.

Acknowledgements

The authors would like to thank the organisations that provided them with the network statistics. The authors would also like to thank the anonymous reviewers for their comments and suggestions.

References

deBry, R., Hastings, T., Herriot, R., Issaacson, S. and Powell P. (1999) *The Internet Printing Protocol/1.0: Model and Semantics*, RFC 2566/2911, IETF.

FX, kim0, (2002) *Attacking Networked Embedded Systems*, Phenoelit, [online, accessed 14May2003], http://www.phenoelit.de/

Fyodor, (2003) Network Mapper, [online, accessed 14May2003], http://www.insecure.org/

Hewlett Packard, (1997), *Printer Job Language Technical Reference Manual*, Hewlett-Packard part number 5021-0380, USA, 10th edition

Hewlett Packard, (2003) JetDirect *Print Servers - HP Jetdirect Port Numbers for TCP and/or UDP Connections*, [online, accessed 14May2003], http://www.hp.com/cposupport/networking/support_doc/bpj01014.html

McLaughlin, L. (1990) *Line Printer Daemon Protocol*, RFC 1179, IETF.

Mudge, (2001) HP Printer display tool, [online, accessed 14May2003], http://www.atstake.com/research/tools/network_utilities/

Valli, C. (2003) The New Homeland Defence, European Conference on Information Warfare and Security, MCIL, Reading, pp143-147.

Vogt, J. (2003) Network Mapper for Windows, [online, accessed 14May2003], http://www.nmapwin.org/